Slovenská technická univerzita v Bratislave
Fakulta elektrotechniky a informatiky
Katedra telekomunikácií

Analýza bezpečnosti štandardu IEEE 802.11

Matej Šustr

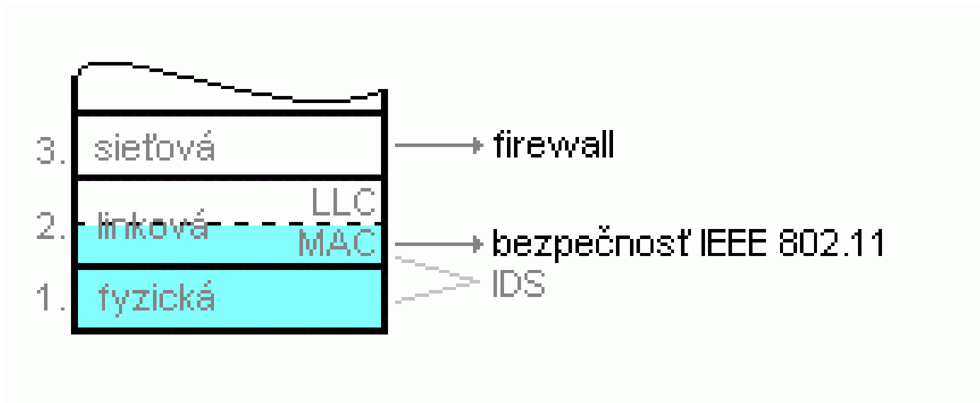
Vedúci diplomovej práce: Ing. Martin Rakús, PhD.

Jún 2007

Prezentácia

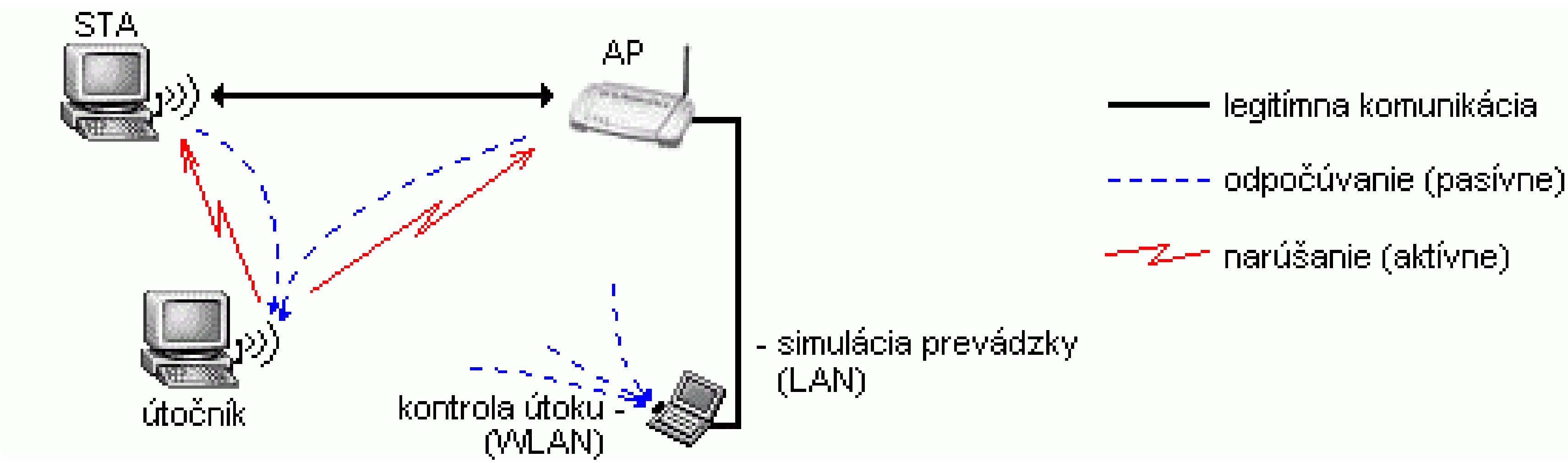
- Úvod do bezpečnosti IEEE 802.11
- Prvky zabezpečenia a útoky voči nim
  - Skryté SSID, Filtrovanie MAC
  - WEP
  - WPA, WPA2
- Ďalšie útoky
  - Man-in-the-middle
  - Útoky na chyby implementácie
  - DoS
- Doplnková ochrana

IEEE 802.11



- fyzická vrstva (PHY) – voľné pásmo
- MAC podvrstva linkovej vrstvy
  - management rámce nie sú nijak zabezpečené

Testovacie zapojenie



- Micronet SP917G Access Point
- Micronet SP906GK
- MSI US54G (ovládač rt2570)
- Asus WL-107G (ovládač rt2500)

Softvér

- GNU/Linux
- ovládače podporujúce režim monitor
- WireShark (pasívne)
- AirSnort (pasívne)
- coWPAtty (pasívne)
- Aircrack-ng (aktívne)
- Aircrack-ptw (aktívne)
- framespam (aktívne)

Zistenie skrytého SSID

- Asociačný rámec obsahuje SSID
  - v otvorenej forme

No.	Time	Source	Destination	Protocol	Info
107	2.773840	Micronet_0b:22:0c	Micronet_07:00:14	IEEE 8	Association Request,SN=1070,FN=0, SSID: "testt"
108	2.774256		Micronet_0b:22:0c	IEEE 8	Acknowledgement

a) počkáme na reasociáciu ľubovoľnej stanice (pasívne: min. až hod.)

b) vnútime disasociáciu/deautentifikáciu niektorej stanici (aktívne: sek.)

Falšovanie MAC adresy

- MAC adresa sa prenáša v otvorenej forme
  - platné adresy sú ľahko zistiteľné
  - integrita zabezpečená až vo WPA

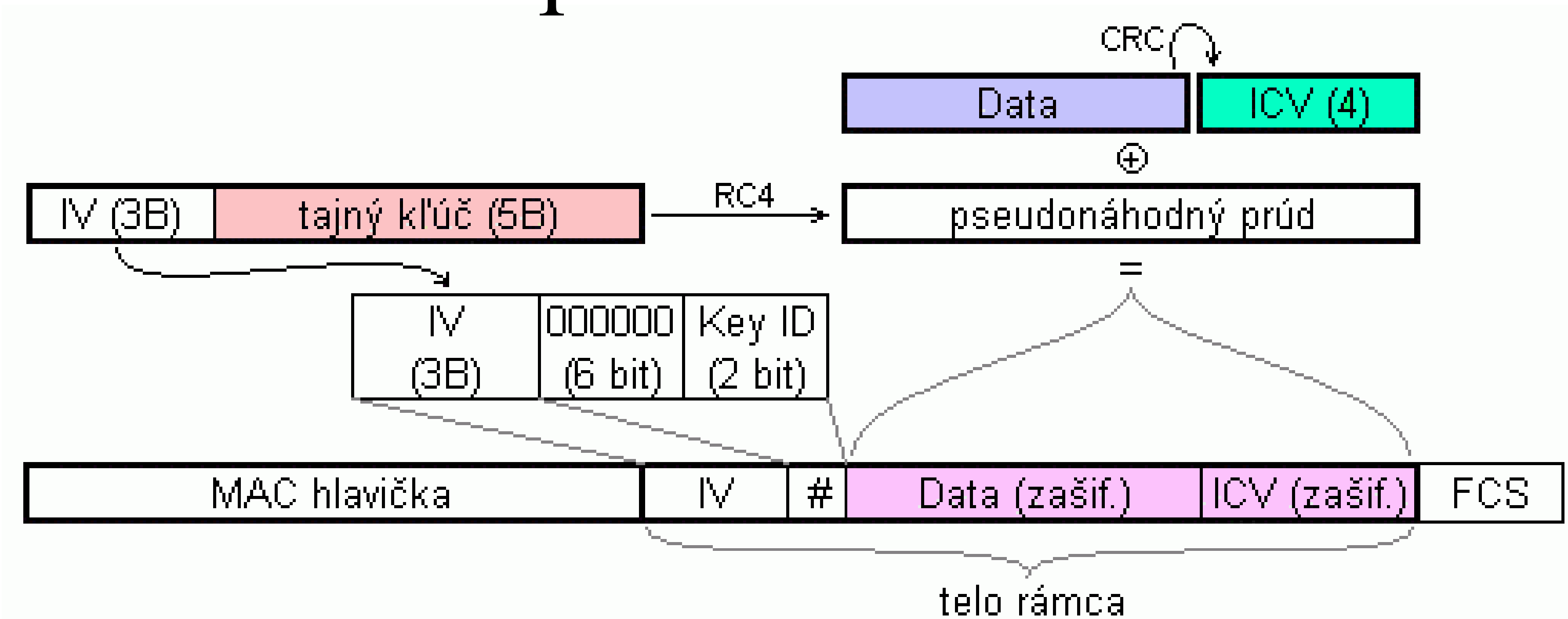
a) zmena umožnená ovládačom (sek.):

```
# ifconfig rausb0 hw ether 00:11:22:33:44:55
#
```

b) posielanie zostrojených rámcov (sek.)

c) preposielanie pozmenených rámcov (sek.)

Enkapsulácia vo WEP



- statický kľúč, opakovanie IV
- linearita CRC-32 a operácie XOR
- slabá šifra RC4, použitá aj pre autentifikáciu

Útoky na WEP

- brute-force 40-bit kľúča (do 34 hod.)
- reinjekcia rámcov (obratom)
- zbieranie slovníka (hodiny až dni, týždne)
- indukčné útoky Arbaugh a chopchop (min.)
- fragmentačný útok (obratom)
- FMS a KoreK (3-6 min. až desiatky minút)
- Klein (1-5 min., dni)

Obrana voči útokom na WEP

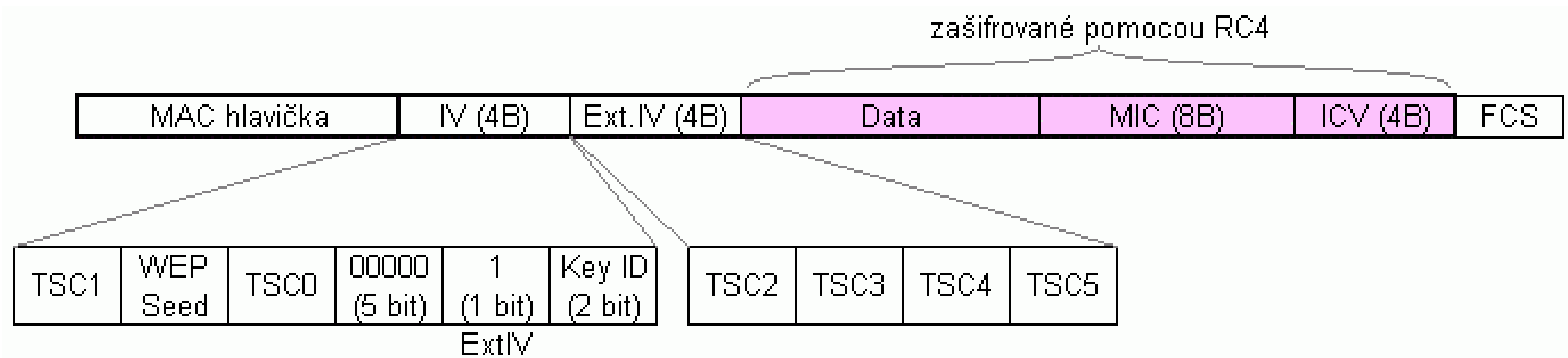
- použitie 104-bit kľúča (admin.) – zabráni brute-force
- otvorená autentifikácia (admin.)
  - obmedzí zbieranie slovníka
- zahadzovanie krátkych rámcov (ovládače, firmware, IDS)
  - zabráni chopchop a fragmentačnému útoku
- ochrana voči reinjekcii (ovládače, firmware, IDS)
  - môže zabrániť aktívnym útokom, alebo ich spomaliť
- statické ARP tabuľky (admin.)
  - obmedzí reinjekciu, Kleinov útok
- použitie WEPplus (admin.) – zabráni FMS
- použitie TKIP, CCMP (WPA/WPA2) (admin.)

Wi-Fi Protected Access

použitie	**WPA**	**WPA2**
Enterprise - vládne inštitúcie - firmy - školstvo	Autentifikácia: **IEEE 802.1x/EAP** Šifrovanie/integrita: **TKIP/Michael**	Autentifikácia: **IEEE 802.1x/EAP** Šifrovanie/integrita: **AES-CCMP**
Personal - domácnosť - malá firma	Autentifikácia: **PSK** Šifrovanie/integrita: **TKIP/Michael**	Autentifikácia: **PSK** Šifrovanie/integrita: **AES-CCMP**

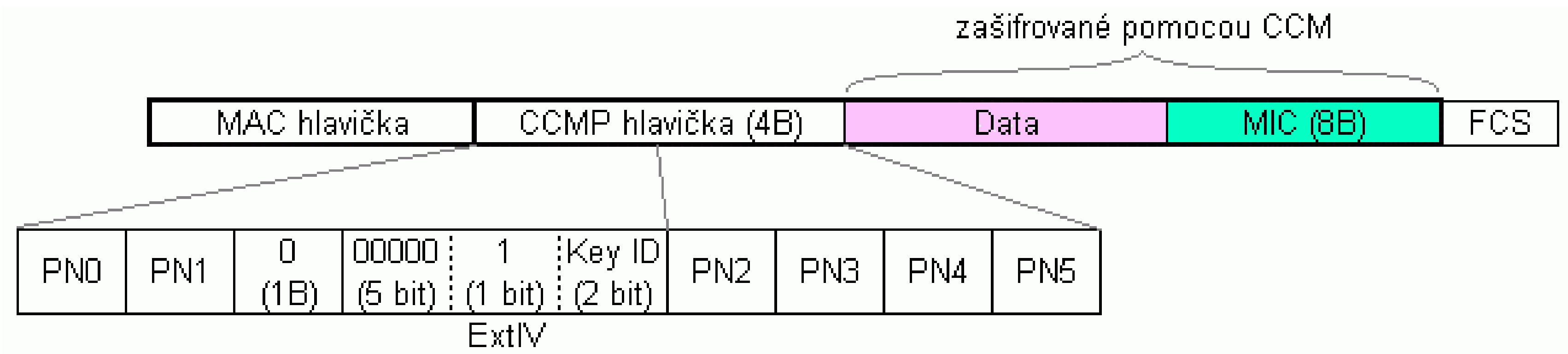
- problémy s kompatibilitou zariadení
  - Wi-Fi certifikácia zaručuje kompatibilitu

Enkapsulácia v TKIP



- implementovateľné na pôvodnom RC4 hardvéri
- kľúč pre RC4 sa mení
- opakovaniu zamedzené pomocou počítadla TSC
- integrita zabezpečená nelineárnym MIC

Enkapsulácia v CCMP



- AES v Counter-Mode/CBC-MAC
- kľúč sa mení
- opakovaniu zamedzené pomocou počítadla PN
- integrita zabezpečená nelineárnym MIC

IEEE 802.1x/EAP

– výmena kľúčov (EAPOL) a autentifikácia

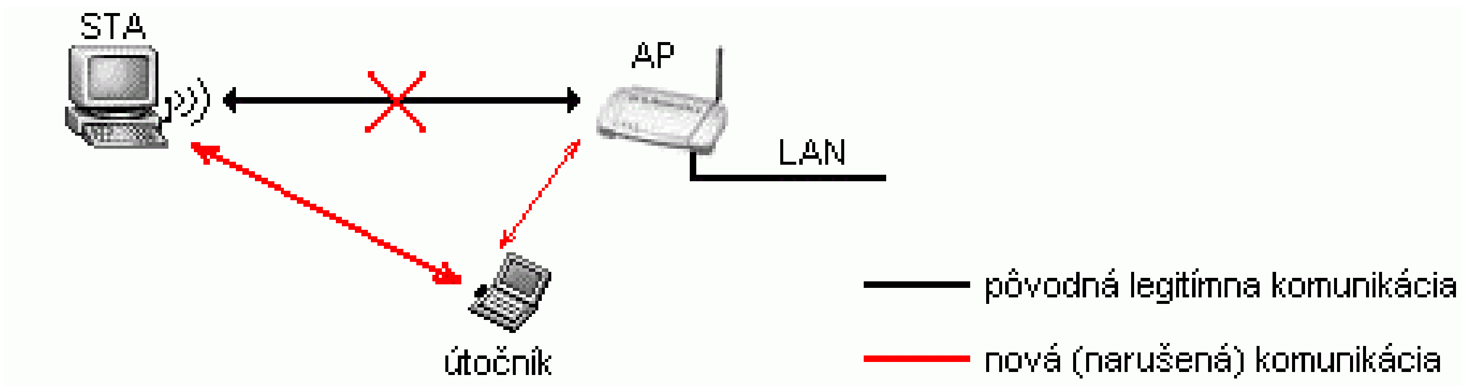
- Wi-Fi certifikované:
  - EAP-TLS
  - EAP-TTLS-MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-SIM
- iné:
  - EAP-MD5
  - EAP-TTLS-PAP, EAP-TTLS-MD5, ...
  - Cisco LEAP

Útoky na WPA a WPA2

– zamerané na výmenu kľúčov (EAPOL), nie na samotné šifrovanie

- slovníkový útok na PSK (minúty pri predvypočítanom postačujúcom slovníku)
- slovníkový útok na Cisco LEAP (min.)
- man-in-the-middle útoky na iné EAP (sek. až hod.)

Man-in-the-middle (aktívne)



- falošné AP na rovnakom alebo inom kanáli
- DoS na pôvodné spojenie
- umožní:
  - „pharming"
  - ukradnutie identity pri EAP-TTLS-*
  - narušenie bezpečnosti vyšších protokolov

„Bezpečné“ WPA/WPA2

- použitie silného PSK (admin.)
  - vhodné len pre „Personal“ použitie
- Wi-Fi Protected Setup (výrobca)
  - navrhnuté pre „Personal“ použitie
- EAP-TLS, EAP-TTLS s overovaním autenticity AP (admin.)
  - v „Enterprise“ prostredí nutnosť

Chyby implementácie

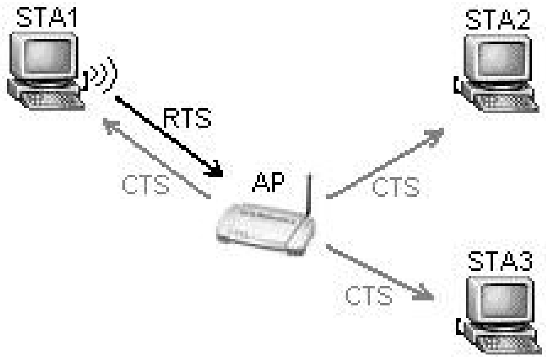
– chyby v ovládačoch (alebo vo firmware)

- buffer overflow (sekundy pri známej chybe)
  – možné aj vykonanie kódu
  – obrana: používanie bezchybných ovládačov (výrobca, admin.)
- vzdialený fingerprinting (sek. až min.)
  – výber vhodného cieľa na konkrétny útok
  – informácie o topológii siete

Denial of Service (aktívne)

- rušenie pásma (hardvérovo náročné)
- PLME_DSSSTESTMODE
  - prístupné len v staršom hardvéri, ovplyvňuje iba 802.11, 802.11b
- RTS/CTS rámce
- deautentifikácia
- zahlcovanie asociačných tabuliek
- spotvorené rámce (trvalé následky)

DoS pomocou CTS





- potreba RTS/CTS vyplýva zo skrytých uzlov
- sto 10-bajtových rámcov za sekundu úplne vyradí všetky uzly v rádiovom dosahu (Duration=32000):

```
# echo -en "\0304\0\0\0175\01\02\03\04\05\06" | framespam -i rausb0

Frame Spammer
Copyright (c) 2007, Matej Sustr

Info      : Sending many frames (delay 10000 us)
......
```

Obrana voči DoS

- fyzická nedostupnosť
- používanie IEEE 802.11a alebo 802.11g v nezmiešanom režime (admin.)
  - zabráni útoku pomocou PLME_DSSSTESTMODE
- stanovenie maximálnej rozumnej hodnoty Duration pre RTS/CTS (štandard, firmware)
- oneskorená deautentifikácia (štandard, firmware, ovládače)
- zabezpečené management rámce – IEEE 802.11w (štd.)
- promptné uvoľňovanie zahltených tabuliek (firmw., ovl.)
- bezchybná implementácia (firmware, ovládače)
- použitie IDS (admin.) – informatívne

Doplnková ochrana (admin.)

- VPN – nutnosť vzájomného overovania
- IPsec
- bezpečné vyššie protokoly (SSH, SSL)
- Wireless IDS

Zhrnutie

- aj slabé zabezpečenie je lepšie ako žiadne
- WEP je slabé zabezpečenie
- pre WPA-PSK treba silné heslo
- pre WPA-EAP treba vzájomné overovanie
- certifikácia Wi-Fi zaručuje kompatibilitu
- potreba aktuálneho softvéru
- možnosť DoS → IEEE 802.11 nevhodné pre kritické aplikácie

Ďakujem za pozornosť

Algoritmus RC4

1. Key Scheduling Algorithm (KSA), ktorým sa na základe vstupného kľúča inicializuje pole S (tzv. S-box), v prípade WEP je veľké 256 bajtov:

```
inicializácia: for i = 0 ... N-1
                    S[i] = i
               j = 0
scramblovanie: for i = 0 ... N-1
                    j = j + S[i] + K[i mod l]
                    vymeň S[i] <-> S[j]
```

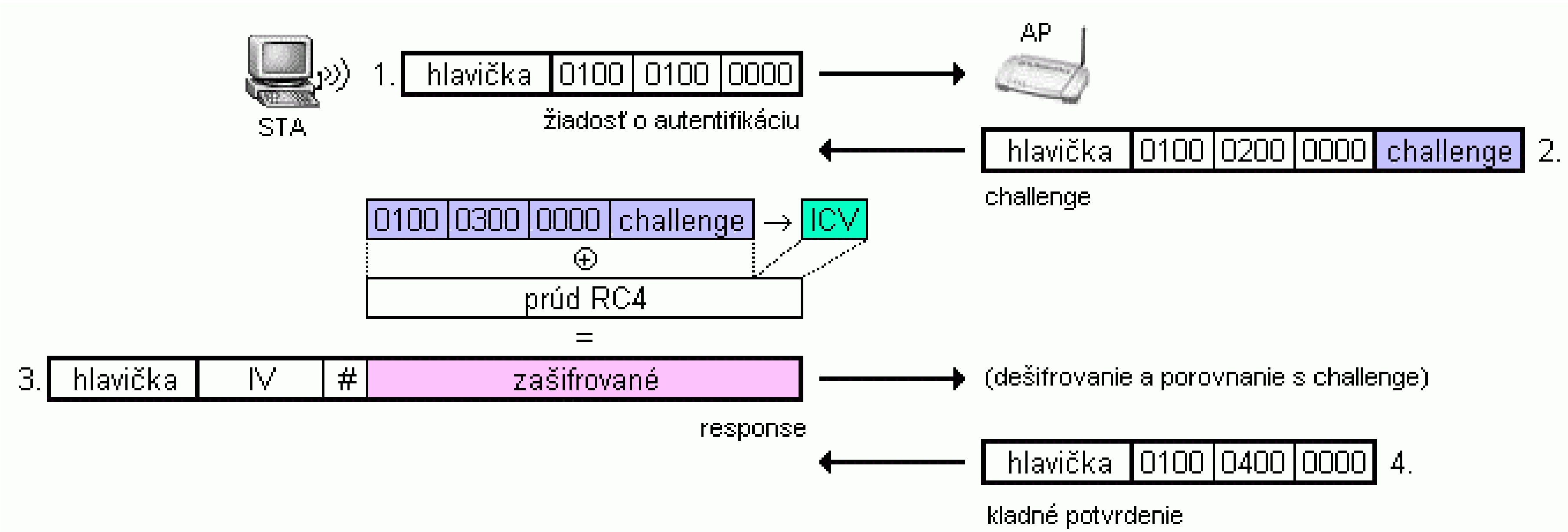
   Kde i, j sú počítadlá, N=256, K je vstupný kľúč, l jeho dĺžka, S je vnútorné stavové pole.

2. Pseudo-Random Generation Algorithm (PRGA), ktorý pomocou poľa S generuje výstupný prúd bajtov:

```
inicializácia: j = 0
generovanie:   for i = 1 ... L
                    j = j + S[i]
                    vymeň S[i] <-> S[j]
                    výstupný bajt = S[S[i] + S[j]]
```

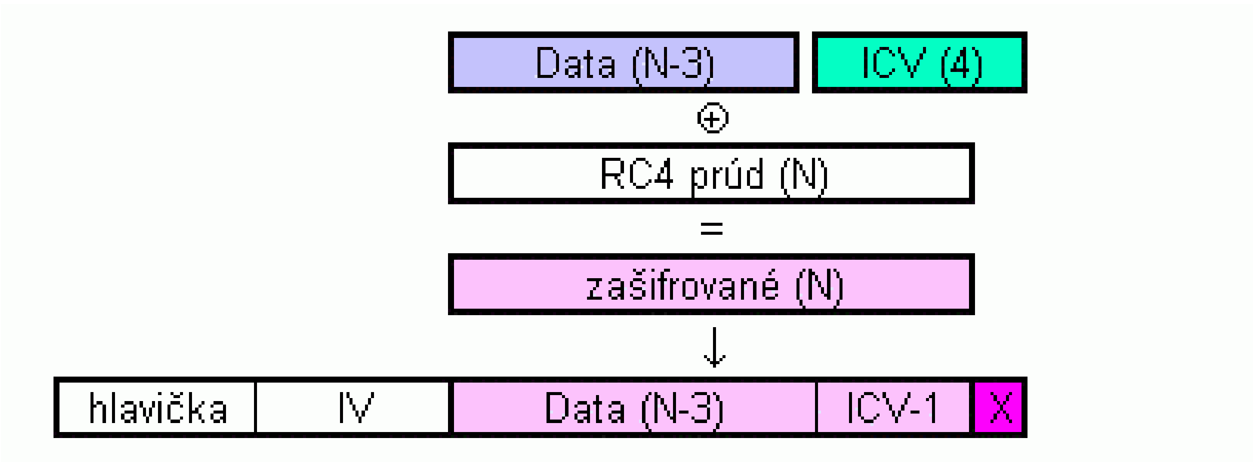
   Kde i, j sú počítadlá, N=256, L je požad. dĺžka výst.prúdu, S je vnútorné stavové pole.

Zbieranie slovníka WEP pomocou Shared-Key autentifikácie



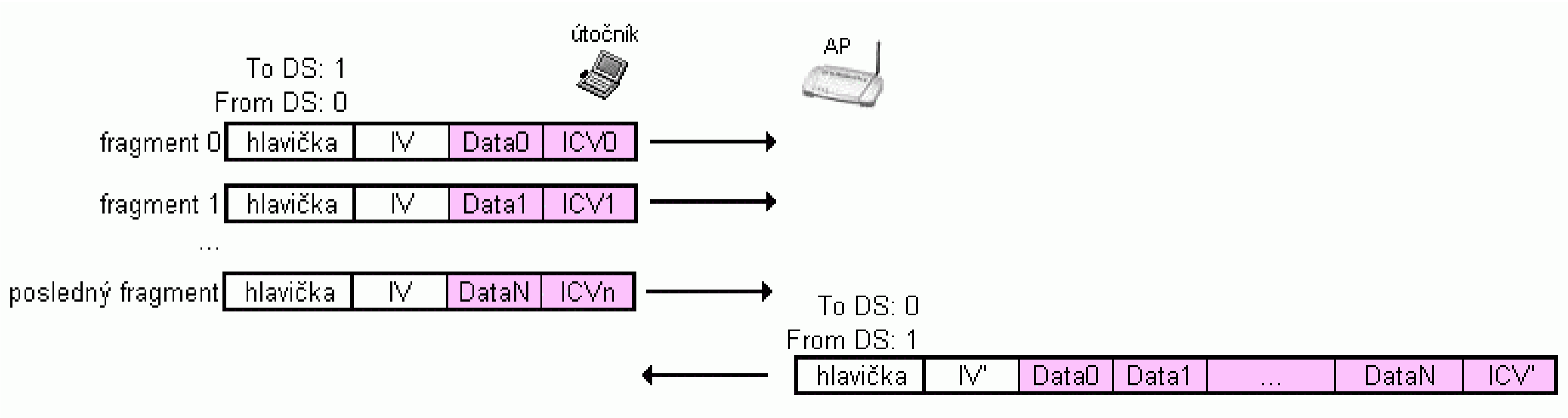
- známy otvorený text (odchytený 2. rámec)
- známy zašifrovaný text (odchytený 3. rámec)
- zistíme prúd RC4 pre použité IV

Indukčný útok Arbaugh



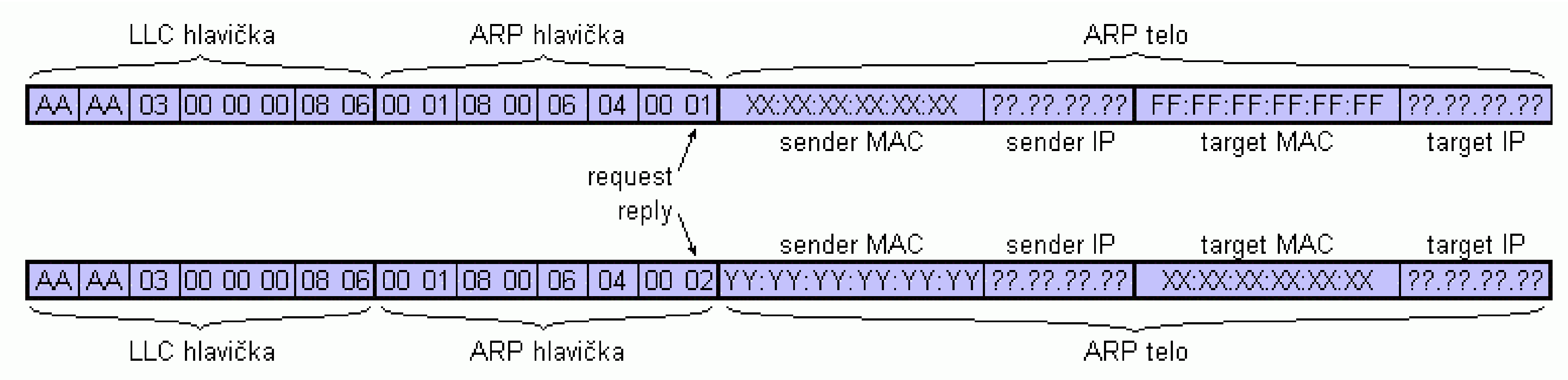
- potreba N známych bajtov RC4 prúdu pre dané IV
- zostrojíme rámec s dátami dĺžky N-3
- vypočítame ICV, použijeme len prvé 3 bajty
- skúšame všetky hodnoty X
- pre platné X vypočítame N+1.-vý bajt RC4 prúdu

Fragmentačný útok



- pre použité IV poznáme K>4 bajtov RC4 prúdu
- pošleme fragmentovanú zašifrovanú správu
- AP ju pospája a prepošle
- získame dlhší RC4 prúd pre nové IV'

Obsah ARP rámcov



- prvých 16 bajtov statických → 16 B známych
- MAC adresy zistiteľné z hlavičky → 28 B
- IP adresy odhadnuteľné → 36 B
- 4-bajtové WEP ICV vypočítateľné → 40 B

Pre-Shared Key

RSA Laboratories: PKCS #5: Password-Based Cryptography Specification

PBKDF2(P=password, S=ssid, c=4096, dkLen=sizeof(PMK)=32)
DK = T1 || T2 || ... || T*l* – *výsledný derivovaný kľúč*

Ti = F (P, S, c, i) – *bloky dĺžky SHA1_MAC_LEN=20*
F(P, S, c, i) = U1 xor U2 xor ... Uc – *xor suma* c *iterácií HMAC_SHA1*
U1 = HMAC_SHA1(P, S || i)
U2 = HMAC_SHA1(P, U1)
Uc = HMAC_SHA1(P, Uc)

HMAC_SHA1(K, T) = SHA1(K xor opad, SHA1(K xor ipad, T))
ipad = bajt 0x36 opakovaný 64 krát
opad = bajt 0x5C opakovaný 64 krát